# Questionário ANBIMA de Due Diligence para Contratação de Terceiros e Serviços em Nuvem

**Contratado:**

**Contratante:**

**Questionário preenchido por:**

**Data:**

***Disclaimer*:** Ao ser preenchido, este questionário, seus anexos e os documentos compartilhados conjuntamente a ele possuem caráter CONFIDENCIAL e não deverão ser divulgados, tanto pela instituição contratante quanto pela respondente, ou encaminhados a terceiros não autorizados pelas partes envolvidas.

**Versão:** **01/01**

ANBIMA

# Sumário

# Apresentação

Este material é uma iniciativa proposta pelo Grupo Consultivo de Cibersegurança com o objetivo de auxiliar instituições atuantes nos mercados financeiro e de capitais a estruturarem processos de diligência na contratação de serviços de tecnologia e complementa as orientações do *Guia ANBIMA para Contratação de Terceiros e Nuvem*[1] e as regras estruturais previstas no documento de *Regras e Procedimentos de Deveres Básicos*[2]. O questionário busca abordar, minimamente, a adoção de práticas consistentes, objetivas e passíveis de verificação que sejam suficientes não apenas para entender e mensurar os riscos associados à prestação do serviço como também para garantir um padrão aceitável da instituição a ser contratada.

A instituição contratante, observadas suas responsabilidades, poderá adicionar outras questões que julgue relevantes na forma de anexo a esse questionário. A potencial instituição contratada (respondente), no caso de possuir certificações amplamente reconhecidas para as práticas e processos abordados no questionário, poderá tão somente informar essas certificações como resposta às perguntas a elas relacionadas (descrevendo, quando aplicável, nome da certificação, entidade emissora, número de registro, data de emissão e data de expiração/prazo de validade/prazo para atualização).

Ressalta-se que o questionário preenchido possui caráter confidencial e não deverá ser divulgado pelas partes envolvidas. Adicionalmente, recomenda-se, quando aplicável, às partes envolvidas, a celebração de Acordo de Não Divulgação, ou Termo de Sigilo e Confidencialidade (*Non Disclosure Agreement* – NDA) a fim de prever obrigações sobre a confidencialidade de eventuais documentos compartilhados, dados e/ou informações específicas fornecidos em resposta ao questionário. Na impossibilidade de compartilhamento pela instituição respondente do questionário de um documento específico solicitado, a contratante poderá, alternativamente, solicitar a exibição do documento em audiência privada, sem manutenção de registros, junto a potencial contratada para avaliação desse documento específico.

O questionário deverá ser respondido por profissional com poderes de representação da instituição respondente, e qualquer alteração relativa às respostas enviadas e aos documentos compartilhados após o preenchimento das respostas deverá ser comunicada e encaminhada à instituição contratante em até cinco dias úteis a partir da referida alteração. A instituição contratada poderá, ainda, solicitar à contratante que especifique por quanto tempo e como se dará a manutenção das informações e documentos disponibilizados em resposta ao questionário. Todos os campos devem ser preenchidos. Caso algum campo não seja aplicável à sua instituição, este deve ser preenchido com “N/A”.

**Este questionário entra em vigor em 1 de julho de 2024.**

[1] Disponível em: <https://www.anbima.com.br/data/files/85/60/2A/F9/3B8C4810272519486B2BA2A8/Guia%20para%20Contratacao%20de%20Terceiros%20e%20Nuvem.pdf>.
[2] Disponível em: <https://www.anbima.com.br/data/files/7B/26/D3/CC/507AC810DE3539C8B82BA2A8/2.%20RP%20de%20Deveres%20Basicos_26.12.2023.pdf>.

# 1. Informações cadastrais

| | |
|---|---|
| **1.1** | Razão social. |
| | |
| **1.2** | Nome fantasia, se houver. |
| | |
| **1.3** | É instituição nacional (brasileira) ou estrangeira? |
| | |
| **1.4** | Informar se possui filiais e especificar a quantidade no Brasil e no exterior, se houver. Caso possua filiais no exterior, indicar, ainda, os países onde estão localizadas. |
| | |
| **1.5** | Sede/endereço/país de constituição. |
| | |
| **1.6** | CNPJ. |
| | |
| **1.7** | Data de constituição. |
| | |
| **1.8** | Telefones. |
| | |
| **1.9** | Website. |
| | |
| **1.10** | Nome, cargo, telefone e e-mail do responsável pelo preenchimento do questionário. |
| | |
| **1.11** | Nome e e-mail do responsável pela segurança da informação. |
| | |

| | |
|---|---|
| **1.12** | Nome e e-mail do responsável pela proteção de dados. |
| | |

## 2. Informações institucionais

| | |
|---|---|
| **2.1** | Descrever o modelo de negócio da instituição, incluindo sua base de clientes e os tipos de produtos e serviços oferecidos. |
| | |
| **2.2** | Informar quais são as autoridades regulatórias e autorregulatórias brasileiras em que a instituição possui registro e a que está sujeita. Indicar, quando aplicável, detalhes sobre os registros, tais como nome, data e nº de registro da atividade. |
| | |
| **2.3** | Informar se a instituição é membro de associação de classe brasileira. Em caso positivo, especificar qual(ais). |
| | |
| **2.4** | Informar:<br>I. O nome das pessoas que compõem a alta administração, com participação igual ou superior a 25% (até o beneficiário final);<br>II. O nome e a atividade de pessoas que não constem no inciso acima, mas que exerçam na instituição significativa influência sobre a condução dos negócios (e.g. sócio oculto, conselho consultivo, conselheiro independente); e<br>III. Se algum membro da alta administração ou diretor (ou *managing directors*) é pessoa politicamente exposta (PEP). |
| | |
| **2.5** | Informar se, nos últimos cinco anos, a instituição ou seus sócios/administradores/dirigentes já foram punidos ou respondem por processos sancionadores na autoridade regulatória e/ou supervisora local em relação à atividade contratada, por processos judiciais e/ou administrativos referentes à lavagem de dinheiro, ao financiamento do terrorismo e ao financiamento da proliferação de armas de destruição em massa (LD/FTP) ou por processos judiciais, administrativos ou arbitrais em que a instituição figure no polo passivo e sejam relevantes para a atividade contratada. Em caso positivo, e se não estiver sob sigilo, informar:<br>I. O número do processo;<br>II. Seu status (encerrado/em julgamento/condenação); e<br>III. Um breve relato sobre os processos, incluindo, quando aplicável, valores, bens ou direitos envolvidos. |

| |
|---|

## 3. Recursos Humanos

| | |
|---|---|
| **3.1** | Fornecer organograma, desde a gestão até o nível operacional, da área de segurança da informação/infraestrutura/cibersegurança da instituição, indicando cargos e níveis hierárquicos dos responsáveis por área. |
| | |
| **3.2** | Em adição à questão anterior, indicar se a instituição possui DPO (*Data Protection officer*) e CISO (*Chief Information Security Officer*), se estes profissionais são internos ou terceirizados e se desempenham suas atividades de forma compartilhada com outras ou não. Caso sejam terceirizados, incluir o nome da empresa que presta o serviço. |
| | |
| **3.3** | Indicar o número total de profissionais da instituição. |
| | |
| **3.4** | Informar se a instituição possui processo de qualificação e treinamento para seus profissionais e para os prestadores de serviço contratados, referente aos assuntos especificados nos itens abaixo. Em caso positivo, descrever resumidamente os procedimentos adotados, como são mantidos os registros dos treinamentos, a periodicidade em que são aplicados e os materiais utilizados (quando aplicável, anexar ao final do questionário). Em caso negativo, justificar e informar se há previsão de implementação de um processo nesse sentido.<br>I. Anticorrupção;<br>II. Conteúdo do código de ética;<br>III. Controles internos e compliance;<br>IV. Anticorrupção e prevenção a lavagem de dinheiro e financiamento ao terrorismo (PLDFT); e<br>V. Segurança da informação / cibernética. |
| | |

## 4. Estrutura, políticas, procedimentos e controles

| | |
|---|---|
| **4.1** | Assinale os tipos de serviço utilizados pela instituição. |

| | |
|---|---|
| Nuvem: SaaS [ ] PaaS [ ] IaaS [ ]<br><br>Consultoria [ ]<br><br>Serviços gerenciados [ ]<br><br>Suporte [ ]<br><br>Outros: especificar. | |
| **4.2** | Assinale quais dados serão processados e/ou armazenados nos serviços especificados na questão anterior. |
| **Processamento:** transacionais [ ] pessoais [ ] pessoais sensíveis [ ]<br><br>**Armazenamento:** transacionais [ ] pessoais [ ] pessoais sensíveis [ ] | |
| **NOTA**<br><br>**Dados transacionais:** informações que rastreiam as interações relacionadas às atividades de uma organização. Normalmente, essas interações são transações comerciais, como pagamentos recebidos de clientes, feitos a fornecedores e movimentação de produtos por meio de estoque, pedidos feitos ou serviços prestados.<br><br>**De acordo com a LGPD:**<br>▪ **Dados pessoais:** informação relacionada com pessoa singular identificada ou identificável. Exemplo.: documento de identificação (RG, CPF etc.), endereço, telefone, entre outros.<br>▪ **Dados sensíveis:** dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização religiosa, filosófica ou política, dados relativos à saúde ou vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa física. | |
| **4.3** | Caso haja tratamento de dados pessoais, acrescentar informações sobre:<br>I. se há a devida coleta e gerenciamento do consentimento do titular;<br>II. se há política de privacidade de dados e termos de uso facilmente disponíveis e acessíveis aos titulares previamente ao pedido do consentimento;<br>III. se há canal específico para receber solicitações do titular, tais como anonimização, pseudonimização, reporte de dados armazenados, alteração ou mesmo deleção de informações;<br>IV. se o canal de atendimento ao titular está pronto para atender as requisições dentro do tempo determinado pela ANPD (agência nacional de proteção de dados); e<br>V. se os devidos mecanismos para a anonimização, pseudonimização, fácil localização, alteração e deleção de informações estão implementadas. |
| | |

| | |
|---|---|
| **4.4** | Informar se há adoção de um plano de contingência. Em caso positivo, indicar se este plano é documentado, submetido a testes periódicos (informar periodicidade), e se possui procedimentos para aprimoramento e correção de eventuais inconsistências. Em caso negativo, justificar e informar se há previsão de implementação de um processo nesse sentido. |
| | |
| **4.5** | Informar se possui Plano de Continuidade de Negócios (PCN) formal e, em caso positivo, informar, no mínimo:<br>I. se é auditado e em qual a periodicidade;<br>II. se é validado/testado por área independente;<br>III. o processo para gerenciamento de crise; e<br>IV. as pessoas de contato/árvore de decisão.<br>Em caso negativo, justificar e informar se há previsão de implementação de um plano nesse sentido. |
| | |
| **4.6** | Informar se possui políticas, programas e procedimentos formais relativos à segurança da informação e cibersegurança. Em caso positivo, indicar se é submetido a testes e/ou auditoria periódicos (informar periodicidade) e apresentar cópia do documento. Em caso negativo, justificar e informar se há previsão de implementação de políticas, programas e procedimentos formais nesse sentido. |
| | |
| **4.7** | Informar se possui plano de resposta a incidente de segurança cibernética. Em caso positivo, apresentar cópia do documento. Em caso negativo, justificar e informar se há previsão de implementação. |
| | |
| **4.8** | Sofreu incidentes de segurança relevantes, com vazamento ou perda de dados, nos últimos 3 anos? Houve alguma notificação? Em caso positivo, detalhar. |
| | |
| **4.9** | Informar se possui contrato explicitando e exigindo requisitos de garantia para confidencialidade, integridade e disponibilidade de dados/informações para outros fornecedores/parceiros com os quais tenha relações de negócio. Em caso positivo, detalhar a cobertura das provisões contratuais. Em caso negativo, justificar. |
| | |
| **4.10** | Informar se possui política e/ou procedimento de *backup* e redundância de informações? Em caso positivo, apresentar cópia do documento e informar o tempo estimado para realização do procedimento. Em caso negativo, justificar e informar se há previsão de implementação. |
| | |

| | |
|---|---|
| **4.11** | Informar se realiza testes periódicos de *restore* do *backup*. Em caso positivo, informar a periodicidade e apresentar registro do último teste executado. Em caso negativo, justificar. |
| | |
| **4.12** | Informar se possui *data center* alternativo para a recuperação do ambiente tecnológico e de dados, em caso de indisponibilidade do principal. Em caso positivo, detalhar as características desse *data center* secundário e o tempo estimado para reinicialização dos serviços. Em caso negativo, justificar. |
| | |
| **4.13** | Informar se possui mecanismos de proteção de dados, por exemplo: antispam, firewall, sistema antivírus, antiphishing, EDR (*Endpoint Detection and Response*), DLP (*Data Loss Prevention*), SIEM (Security Information and Event Management) e WAPP (*Web APP and API Protection*)? Em caso positivo, detalhar. Em caso negativo, justificar. |
| | |
| **4.14** | Informar se utilizará armazenamento, processamento e gerenciamento de dados no exterior durante a prestação de serviços. Em caso positivo, indicar países/localização geográfica. |
| | |
| **4.15** | Descrever as ferramentas e/ou os mecanismos utilizados para a proteção dos dados transacionados entre a contratante e a contratada. |
| | |
| **4.16** | Descrever as práticas adotadas na detecção de atividades não autorizadas e de situações acidentais ou ilícitas de destruição, perda, alteração ou qualquer outra forma nos sistemas utilizados na prestação de serviços. Indicar um responsável, bem como a área e o reporte. |
| | |
| **4.17** | Descrever os canais de gestão utilizados em caso de detecção de incidente de cibersegurança, bem como o prazo de registro. Informar se há comunicação a clientes e/ou reguladores. |
| | |
| **4.18** | Informar se a instituição realiza testes periódicos de verificação de segurança e integridade de sistemas. Em caso positivo, indicar periodicidade. Em caso negativo, justificar. |
| | |
| **4.19** | Informar se possui plano(s) de ação recente (implementado no último ano) decorrente de avaliação de risco, testes de controles internos ou de auditoria relacionado(s) à segurança da informação e cibersegurança. |

| | |
|---|---|
| | |
| **4.20** | Informar se possui gestão de vulnerabilidades. Em caso positivo, detalhar. Em caso negativo, justificar. |
| | |
| **4.21** | Caso possua plataforma de serviços, informar se aplica múltiplos fatores de autenticação. Em caso positivo, descrever os métodos de autenticação e os mecanismos de acesso secundário ou recuperação de acesso (no caso de perda do dispositivo/aplicação responsável pelo segundo fator de autenticação). Em caso negativo, justificar.<br><br>Adicionalmente, informar:<br>I. se a aplicação é compatível com SSO – *Single Sign-on* e, em caso positivo, descrever métodos de sincronização para autenticação; e<br>II. se aplicação permite a restrição de acesso a IPs específicos. |
| | |
| **4.22** | Informar se possui processos de criptografia de dados em repouso e em trânsito. Em caso positivo, detalhar e descrever a tecnologia utilizada. Em caso negativo, justificar. |
| | |

## 5. Compliance e controles internos

| | |
|---|---|
| **5.1** | Informar se possui área própria de controles internos e conformidade das regras, políticas e regulação (*Compliance*)? Em caso positivo, fornecer organograma, desde a gestão até o nível operacional, indicando cargos e níveis hierárquicos. Em caso negativo, informar se contrata terceiros para desempenhar esta(s) atividade(s) e, caso aplicável, indicar o nome da empresa que fornecedora. |
| | |
| **5.2** | Descrever se a instituição utiliza algum sistema para execução das atividades de compliance e controles internos. |
| | |
| **5.3** | Informar se possui comitê de controles internos e compliance. Em caso positivo, informar:<br>I. Periodicidade;<br>II. Composição;<br>III. Linhas de reporte;<br>IV. Principais diretrizes; e<br>V. Se as decisões são formalizadas.<br>Em caso negativo, justificar e informar se há previsão de implementação. |

| | |
|---|---|
| | |
| **5.4** | Anexar o código de ética e conduta de instituição e informar se há adesão formal pelos profissionais. |
| | |
| **5.5** | Descrever a estrutura da instituição para disponibilização de canal de comunicação por meio do qual os funcionários, colaboradores, clientes, usuários, parceiros ou fornecedores possam reportar, sem a necessidade de se identificarem, situações com indícios de ilicitude de qualquer natureza, relacionadas às atividades da instituição. |
| | |

## 6. Informações Gerais (PLD/FTP)

| | |
|---|---|
| **6.1** | A instituição possui questionário Wolfsberg? Em caso positivo, anexar.<br>As instituições poderão, em comum acordo, considerar o questionário Wolfsberg como substitutivo às seções 7, 8 e 9 deste questionário. |
| | |

## 7. Programa de PLD/FTP

| | |
|---|---|
| **7.1** | Anexar a política de PLD/FTP da instituição e informar:<br>I. se a política é aplicada a todas as filiais e subsidiárias no país de origem e no exterior, caso aplicável;<br>II. a governança de aprovação da política e periodicidade para sua revisão; e<br>III. se for gestor de recursos, incluir, caso não conste na política, o processo de PLD/FTP adotado para os ativos que integram os fundos de investimento e as carteiras administradas. |
| | |
| **7.2** | Informar se dispõe de estrutura de PLD/FTP autônoma e independente das áreas de negócios e a governança aplicável, incluindo organograma, desde a gestão até o nível operacional, indicando cargos e níveis hierárquicos. |
| | |

| | |
|---|---|
| **7.3** | Informar se possui comitê ou organismo que trate de PLD/FTP. Em caso positivo, informar:<br>I. periodicidade em que é realizado;<br>II. áreas envolvidas, cargo dos membros e número de participantes; e<br>III. se as decisões são formalizadas. |
| | |
| **7.4** | Informar quantos funcionários são dedicados à atividade de PLD/FTP. |
| | |
| **7.5** | Informar há quanto tempo o diretor de PLD/FTP exerce suas funções na instituição e se este exerce outra atividade na instituição. Em caso positivo, indicar qual(is) atividade(s). |
| | |
| **7.6** | Informar se a alta administração recebe, sem prejuízo do prazo previsto na regulação vigente, relatórios sobre a situação do programa de PLD/FTP. Em caso positivo, indicar a periodicidade. |
| | |
| **7.7** | Informar se possui procedimentos de conheça seu colaborador (*Know Your Employee – KYE*). Em caso positivo, descrever como é feito e a periodicidade de revisão, ou indicar o item que trata desse assunto na política de PLD/FTP. Em caso negativo, justificar e informar se há previsão de implementação. |
| | |
| **7.8** | Informar se utiliza terceiros ou sistemas contratados para realizar quaisquer dos componentes do seu programa de PLD/FTP. Em caso positivo, indicar e descrever brevemente. |
| | |
| **7.9** | Nos termos do item acima, caso a instituição utilize terceiros ou sistemas contratados para realizar quaisquer dos componentes do seu programa de PLD/FTP, indicar as regras adotadas para contratação e monitoramento desse terceiro. |
| | |
| **7.10** | Informar se possui programa de treinamento inicial e de reciclagem de PLD/FTP. Em caso positivo, descrever, minimamente:<br>I. a abrangência, incluindo como se dá o treinamento para os prestadores de serviço e prepostos, caso aplicável;<br>II. a periodicidade;<br>III. se utiliza algum sistema;<br>IV. se é solicitada prova ao final para testar o conhecimento; e |

| | |
|---|---|
| | V. se há registro e armazenamento dos treinamentos realizados.<br>Em caso negativo, justificar e informar se há previsão de implementação. |
| | |
| **7.11** | Informar se possui monitoramento periódico em seu programa de PLD/FTP. Em caso positivo, indicar a periodicidade e detalhar o procedimento adotado quando são detectadas inconsistências. Em caso negativo, justificar e informar se há previsão de implementação. |
| | |
| **7.12** | Informar se realiza testes em seu programa de PLD/FTP utilizando área independente (e.g. auditoria interna ou externa, área de controles internos, compliance ou gerenciamento de riscos). Em caso positivo, indicar a periodicidade e detalhar a governança para recebimento do resultado e as práticas adotadas para tratativa dos apontamentos (plano de ação). Em caso negativo, justificar e informar se há previsão de implementação. |
| | |
| **7.13** | Detalhar como se mantém em conformidade com práticas e/ou políticas anticorrupção, em linha com as exigências regulatórias, e anexar documento que formalize essas práticas e/ou políticas. |
| | |
| **7.14** | Informar se possui canal de denúncia anônimo para acolher as ocorrências referentes a desvios éticos, de conduta, suspeita de ilícitos e corrupção. Em caso positivo, descrever quais são os critérios de acesso e de governança no tratamento das denúncias. Em caso negativo, justificar e informar se há previsão de implementação. |
| | |
| **7.15** | Informar se realiza atividades e/ou negócios no mercado de moedas virtuais ou criptoativos. Em caso positivo, detalhar as atividades e/ou negócios e como se dá o controle de PLD/FTP. |
| | |

# 8. Conheça seu cliente

| | |
|---|---|
| **8.1** | Informar o procedimento de Conheça seu Cliente (*Know Your Customer – KYC*) adotado pela instituição e detalhar, minimamente:<br>I. o processo de identificação do cliente, até o beneficiário final (quando aplicável);<br>a. indicar se o processo de identificação do cliente é físico ou digital; e<br>b. caso o processo de identificação do cliente seja digital, detalhar como é feita a conferência da identidade do cliente e mencionar os mecanismos utilizados, caso aplicável;<br>II. o processo de qualificação do cliente, quando aplicável;<br>III. como se dá a identificação de PEP, bem como seus familiares e estreitos colaboradores (PEP relacionado) e organização sem fins lucrativos;<br>IV. como se dá a condução de diligências devidas, incluindo validação das informações recebidas (se são feitas consultas em *bureaus* internos ou externos);<br>V. se há previsão de visitas presenciais a seus clientes (PF ou PJ);<br>VI. o processo de *onboarding* do cliente e informar se há prazo pré-estabelecido para conclusão e se existe política de alçada/exceção;<br>VII. o processo de aprovação adotado para os clientes de maior risco e o tratamento dado após a aprovação, caso aplicável;<br>VIII. os procedimentos de revisão cadastral;<br>IX. os procedimentos de revisão do processo de KYC;<br>X. o nível de diligência adotado para identificar informações reputacionais relacionadas a PLD/FTP, se o processo é manual ou feito por meio de algum sistema (próprio ou de terceiros) e como isso retroalimenta os processos de KYC da instituição; e<br>XI. o registro de todas as operações realizadas pelos clientes, assim como dos produtos e serviços contratados, conforme legislação vigente. |
| | |
| **8.2** | Informar o procedimento adotado pela instituição para obter as informações abaixo dos clientes.<br>I. Atividade;<br>II. Capacidade financeira;<br>III. Origem do patrimônio e dos recursos;<br>IV. Localização geográfica;<br>V. Modelo de negócio, se aplicável;<br>VI. Produtos, serviços, operações, transações e canais de distribuição utilizados;<br>VII. Contraparte das operações realizadas em nome do cliente, no caso de operações realizadas em ambientes de registro; |

| | |
|---|---|
| | VIII. Risco jurídico, reputacional e socioambiental para a instituição;<br>IX. Relacionamento com outros prestadores de serviço, inclusive, as políticas de PLD/FTP de tais prestadores; e<br>X. Informações adversas (especificar).<br>Indicar os critérios não considerados e justificar a não utilização. Adicionalmente, quando aplicável, detalhar as diligências adotadas para obtenção de informações que podem ser fornecidas após o início ou durante o relacionamento e as consequências de não obtenção. |
| | |
| **8.3** | Informar o processo adotado pela instituição para consultar listas restritivas. Descrever, minimamente:<br>I. se a consulta é manual ou automatizada;<br>II. quais são as listas consultadas; e<br>III. qual periodicidade. |
| | |

## 9. Monitoramento e comunicação às autoridades

| | |
|---|---|
| **9.1** | Informar qual o monitoramento adotado para os clientes de maior risco, destacadamente na condição de PEP e de organização sem fins lucrativos. |
| | |
| **9.2** | Informar qual procedimento adotado pela instituição caso seja identificado, no curso do relacionamento com o cliente, que se trata de PEP ou organização sem fins lucrativos. |
| | |
| **9.3** | Informar qual área faz a comunicação ao órgão responsável pelo monitoramento e combate aos crimes financeiros e a governança adotada pela instituição nesse processo (instância de aprovação, se aplicável). |
| | |
| **9.4** | Informar quais são os procedimentos utilizados pela instituição para monitorar transações de atividades atípicas (propostas ou realizadas). Detalhar se utiliza sistema automatizado (indicar fornecedor) ou se é manual. |
| | |
| **9.5** | A partir da identificação de atividades atípicas, informar se possui procedimentos para revisá-las e qualificá-las como suspeitas. Adicionalmente, descreva as providências a serem adotadas nestes casos. |

| | |
|---|---|
| | |
| **9.6** | Indicar quais os procedimentos adotados pela instituição para cumprir com as medidas estabelecidas nas resoluções sancionatórias do Conselho de Segurança das Nações Unidas (CSNU), nos termos da regulamentação vigente. Indicar como é realizado o monitoramento desses procedimentos. |
| | |
| **9.7** | Informar como a instituição realiza o bloqueio dos ativos, nos termos solicitados pelo CSNU. |
| | |
| **9.8** | Informar qual processo adotado nos últimos 5 anos para manter o histórico de reporte ao Conselho de Controle de Atividades Financeiras (COAF). |
| | |

## 10. Gerenciamento de risco

| | |
|---|---|
| **10.1** | Informar se possui área(s) própria(s) de gerenciamento de riscos ou se contrata terceiros para desempenhar essa atividade. Neste caso, informe o nome e descreva a experiência do contratado e a forma de supervisão. |
| | |
| **10.2** | Informar qual sistema de controle de risco é adotado pela instituição. |
| | |
| **10.3** | Informar se possui comitê de gerenciamento de riscos. Em caso positivo, informar:<br>I. periodicidade em que é realizado;<br>II. áreas envolvidas e número de participantes; e<br>III. se as decisões são formalizadas. |
| | |

## 11. Jurídico

| | |
|---|---|
| **11.1** | Informar se possui departamento jurídico próprio. Em caso positivo, indicar a composição da área. Em caso negativo, informar se contrata terceiros para essa atividade e detalhar minimamente o escopo da contratação e indicar o nome da instituição contratada. |

| |
|---|
| |

## 12. Outros

| | |
|---|---|
| 12.1 | Informar se a instituição possui uma apólice de seguro de responsabilidade. Em caso positivo, anexar documento que comprove a contratação da apólice e as informações sobre a cobertura do seguro contratado. Em caso negativo, justificar. |
| | |